



Configuring WEP and WEP Features

This chapter describes how to configure Wired Equivalent Privacy (WEP), Message Integrity Check (MIC), and Temporal Key Integrity Protocol (TKIP). This chapter contains these sections:

- [Understanding WEP, page 9-2](#)
- [Configuring Cipher Suites and WEP, page 9-3](#)

Understanding WEP

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point/bridge can receive the access point/bridge's radio transmissions. Because WEP is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

WEP encryption scrambles the radio communication between access point/bridges to keep the communication private. Communicating access point/bridges use the same WEP key to encrypt and unencrypt radio signals. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to just one device on the network. Multicast messages are addressed to multiple devices on the network.

Extensible Authentication Protocol (EAP) authentication provides dynamic WEP keys to wireless devices. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key. See [Chapter 10, “Configuring Authentication Types”](#) for detailed information on EAP and other authentication types.

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Because cipher suites provide the protection of WEP while also allowing use of authenticated key management, Cisco recommends that you enable WEP by using the **encryption mode cipher** command in the CLI or by using the cipher drop-down menu in the web-browser interface. Cipher suites that contain TKIP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

These security features protect the data traffic on your wireless LAN:

- WEP (Wired Equivalent Privacy)—WEP is an 802.11 standard encryption algorithm originally designed to provide your wireless LAN with the same level of privacy available on a wired LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with reasonable effort.
- TKIP (Temporal Key Integrity Protocol)—TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. TKIP adds four enhancements to WEP:
 - A per-packet key mixing function to defeat weak-key attacks
 - A new IV sequencing discipline to detect replay attacks
 - A cryptographic message integrity Check (MIC), called *Michael*, to detect forgeries such as bit flipping and altering packet source and destination
 - An extension of IV space, to virtually eliminate the need for re-keying
- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- CMIC (Cisco Message Integrity Check)—Like TKIP's *Michael*, Cisco's message integrity check mechanism is designed to detect forgery attacks.



Note

When VLANs are configured on a wireless bridge link, encryption settings such as WEP, MIC, TKIP, and AES apply only to the native VLAN and its assigned SSID.

Configuring Cipher Suites and WEP

These sections describe how to configure cipher suites, WEP and additional WEP features such as MIC and TKIP:

- [Creating WEP Keys, page 9-3](#)
- [Enabling Cipher Suites and WEP, page 9-5](#)

WEP, TKIP, and MIC are disabled by default.

Creating WEP Keys

Beginning in privileged EXEC mode, follow these steps to create a WEP key and set the key properties:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	encryption [vlan <i>vlan-id</i>] key 1-4 size { 40 128 } encryption-key [transmit-key]	Create a WEP key and set up its properties. <ul style="list-style-type: none"> • (Optional) Select the VLAN for which you want to create a key. WEP, MIC, and TKIP are supported only on the native VLAN. • Name the key slot in which this WEP key resides. You can assign up to 4 WEP keys for each VLAN, but key slot 4 is reserved for the session key. • Enter the key and set the size of the key, either 40-bit or 128-bit. 40-bit keys contain 10 hexadecimal digits; 128-bit keys contain 26 hexadecimal digits. • (Optional) Set this key as the transmit key. The key in slot 2 is the transmit key by default. If you enable WEP with MIC, use the same WEP key as the transmit key in the same key slot on both root and non-root access point/bridges.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to create a 128-bit WEP key in slot 2 for VLAN 1 and sets the key as the transmit key:

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 key 2 size 128 12345678901234567890123456
transmit-key
bridge(config-if)# end
```

WEP Key Restrictions

Table 9-1 lists WEP key restrictions based on your security configuration.

Table 9-1 WEP Key Restrictions

Security Configuration	WEP Key Restriction
CCKM or WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP key in key slot 4
Cipher suite with 40-bit WEP	Cannot configure a 128-bit key
Cipher suite with 128-bit WEP	Cannot configure a 40-bit key
Cipher suite with TKIP	Cannot configure any WEP keys
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
Static WEP with MIC or CMIC	Root and non-root access point/bridges must use the same WEP key as the transmit key, and the key must be in the same key slot on both root and non-root access point/bridges

Example WEP Key Setup

Table 9-2 shows an example WEP key setup that would work for the root access point/bridge and an associated non-root access point/bridge:

Table 9-2 WEP Key Setup Example

Key Slot	Root Access Point/Bridge		Associated Non-Root Access Point/Bridge	
	Transmit?	Key Contents	Transmit?	Key Contents
1	x	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	x	09876543210987654321fedcba
3	—	not set	—	not set
4	—	not set	—	FEDCBA09876543211234567890

Because the root access point/bridge's WEP key 1 is selected as the transmit key, WEP key 1 on the non-root access point/bridge must have the same contents. WEP key 4 on the non-root access point/bridge is set, but because it is not selected as the transmit key, WEP key 4 on the root access point/bridge does not need to be set at all.



Note If you enable MIC but you use static WEP (you do not enable any type of EAP authentication), both the root access point/bridge and any non-root access point/bridges with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled root access point/bridge uses the key in slot 1 as the transmit key, a non-root access point/bridge associated to the root access point/bridge must use the same key in its slot 1, and the key in the non-root access point/bridge's slot 1 must be selected as the transmit key.

Enabling Cipher Suites and WEP

Beginning in privileged EXEC mode, follow these steps to enable a cipher suite:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	encryption [vlan <i>vlan-id</i>] mode ciphers {[aes-ccm ckip cmic ckip-cmic tkip]} {[wep128 wep40]}	<p>Enable a cipher suite containing the WEP protection you need. Table 9-3 lists guidelines for selecting a cipher suite that matches the type of authenticated key management you configure.</p> <ul style="list-style-type: none"> (Optional) Select the VLAN for which you want to enable WEP and WEP features. Set the cipher options and WEP level. You can combine TKIP with 128-bit or 40-bit WEP. <p>Note If you enable a cipher suite with two elements (such as TKIP and 128-bit WEP), the second cipher becomes the group cipher.</p> <p>Note You can also use the encryption mode wep command to set up static WEP. However, you should use encryption mode wep only if none of the non-root access point/bridges that associate to the root access point/bridge are capable of key management. See the <i>Cisco IOS Command Reference for Cisco Access Points and Bridges</i> for a detailed description of the encryption mode wep command.</p> <p>Note When you configure TKIP-only cipher encryption (not TKIP + WEP 128 or TKIP + WEP 40) on any radio interface or VLAN, the SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSID, non-root access point/bridge authentication fails on the SSID.</p>
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable a cipher suite.

This example sets up a cipher suite for VLAN 1 that enables CKIP, CMIC, and 128-bit WEP.

```
bridge# configure terminal
bridge(config)# configure interface dot11radio 0
bridge(config-if)# encryption vlan 1 mode ciphers ckip-cmic wep128
bridge(config-if)# end
```

Matching Cipher Suites with WPA

If you configure your access point/bridges to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. [Table 9-3](#) lists the cipher suites that are compatible with WPA and CCKM.

Table 9-3 *Cipher Suites Compatible with WPA and CCKM*

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	<ul style="list-style-type: none"> • encryption mode ciphers wep128 • encryption mode ciphers wep40 • encryption mode ciphers ckip • encryption mode ciphers cmic • encryption mode ciphers ckip-cmic • encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40
WPA	<ul style="list-style-type: none"> • encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40



Note

When you configure **TKIP-only** cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, the SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSID, non-root access point/bridge authentication fails on the SSID.

For a complete description of WPA and CCKM and instructions for configuring authenticated key management, see the [“Using WPA Key Management”](#) section on page 10-5 and the [“Using WPA Key Management”](#) section on page 10-5.